system **130, 140, 150** will be a public encryption key and the central access control system **100** would encrypt the distribution CD's decryption key using the requesting information access system's **130, 140, 150** public key.

If the central access control system **100** is unable to verify the request based on the database within the central access control system **100**, or if it is not supposed to grant the request based on the ARL, the central access control system **100** will not return the decryption key, and instead it will trigger an attempted security breach alert.

If the distribution CD decryption key is sent, the information access system **130, 140, 150** will use it to decrypt the distribution CD and allow the user access to the sensitive information. In an alternative embodiment, the information access system **130, 140, 150** can store the distribution CD decryption key in a key storage area that is only accessible by the user who caused the key to be retrieved. Preferably, the information access system **130, 140, 150** automatically retrieves distribution CD decryption keys from either the central access control system **100** or from the key storage area, and does so transparently to the user.

Turning to FIG. **2**, a block diagram depicting a layout of an embodiment of the disc identification information **200** of the present invention is provided. The central access control system **100** (of FIG. **1**) can track an trace which duplicated CD disc **120** goes to which information access system **130, 140, 150** at a branch office. This tracking and tracing is achieved through the disc identification information **200** recorded directly on the CD media. The program in the central access control system **100** is configured to write to the R–W subchannels of the control bytes of the first sector of a recordable disc. There are **98** control bytes in this sector with the R–W occupying Bit **0** through Bit **5** of each byte. Following the first 2 bytes **210**, there are 64 six bit words available for user data contained within four groups **220, 240, 260, 280** of 24 bytes. There are 16 six bit words within the first group of 24 bytes **220** that are used for central access control system **100** designated Volume numbers **230**, within the next group of 24 bytes **240**, there are 16 six bit words that are used for disc ID numbers **250**, and within the remaining two groups of 24 bytes **260, 280** (48 bytes total) there are 32 six bit words that are used for Serial numbers **270, 290**.

Using the SCSI-3 "WRITE PARAMETER" command, the Volume numbers **230**, the disc ID numbers **250**, and the Serial numbers **270, 290** are recorded in the user data area. In a preferred embodiment, the characters and numbers that are used to represent the disc identification information **200** are taken from the Transcode character set. The transcode character set includes the necessary alphabets (of a number of languages) in upper case, numbers, and some control characters. Use of the Transcode character set eliminates the need to perform shift-pack and shift-unpack of the six bit words when reading and writing to and from the CD media. As described above the disc identification information **200** is used by the information access systems **130, 140, 150** to request decryption keys from the central access control system **100**.

Turning to FIG. **3**, a flow chart depicting the steps of an example embodiment of a method of securely distributing data on a fixed media is provided. In Step **S1**, the data read from the master CD set is encrypted within the central access control system **100** using the multi-disc CDR duplicator **110**. In Step **S2**, the encrypted data is recorded to the distribution CD sets **120** also using the multi-disc CDR duplicator **110**. In Step **S3**, the disc identification information **200** is written to the distribution CDs **120**. In Step **S4**, the disc identification information **200** is stored within the database in the central access control system **100**. In Step **S5**, the distribution CDs **120** are transported to the various remote locations.

In Step **S6**, at a remote location, a distribution CD **120** is loaded into an information access system **130**. In Step **S7**, a user logs into the information access system **130**. In Step **S8**, the disc identification information **200** is read by the information access system **130** from the distribution CD **120**. In Step **S9**, the information access system **130** performs a local database lookup to determine whether a decryption key is present from the currently logged-in user's prior use of the system. The look-up would be performed upon a secure database that relates keys and user login identities that is stored within the information access system **130**. If the decryption key is present within the secure database, the system jumps to Step **S17** where the distribution CD **120** is decrypted. In an alternate embodiment, the information access system **130** could generate a message to the central access control system **100** reporting the request and grant of the locally stored decryption key. If the decryption key is not stored locally, or if a key expiration security mechanism has been set and activated, the system moves to Step **10**. A key expiration security mechanism, if set, would invalidate any stored keys if too much time has passed since the last use of the keys or if an invalid attempt to access stored keys is detected. This mechanism would preferably be implemented as part of the security system of the secure database stored with the information access systems **130, 140, 150**.

In Step **10**, the information access system **130** requests the decryption key by transmitting its remote location identification number (a public key) and the disc identification information **200** to the central access control system **100** via the bi-lateral communications link **132**. Next, in Step **S11**, the central access control system **100**, will attempt to verify the request by performing a database lookup to determine if valid disc identification information **200** has been presented in a correct, predefined format by a valid requester using a valid remote location identification number. If the request cannot be verified, the system moves to Step **S18**, where the request is denied and an attempted security breach alert is triggered and logged. If, on the other hand, the request is verified, the central access control system **100** will next attempt to determine whether the requester is authorized in Step **S12**. Authorization is determined based upon a database lookup of the remote location identification number within the ARL as described above. If the requester is not listed on the ARL, the system moves to Step **S18**, where the request is denied and an attempted security breach alert is triggered and logged. If, on the other hand, the requester is authorized, the system moves to Step **S13**.

In Step **S13**, the requested decryption key is itself encrypted using the remote location identification number of the requester as a public key. In Step **S14**, the encrypted decryption key is transmitted to the requesting information access system **130** via the bi-lateral communication link **132** by the central access control system **100**. Once the encrypted decryption key is received by the information access system **130**, it is decrypted in Step **S15**. In Step **S16**, the decryption key for the distribution CD **120** is stored for future use by the logged-in user. Finally, in Step **S17**, the distribution CD **120** is decrypted.

Various other modifications and alterations in the structure and method of operation of this invention will be apparent to those skilled in the art without departing from the scope and spirit of the invention. Although the invention has been described in connection with specific preferred embodiments, it should be understood that the invention as